# Configuring redundant architecture using two FortiGates and internal switching

The following recipe provides useful instructions for customers with multi-site architecture and redundant firewalls. It is intended for those customers that want to reduce the number of on-site appliances while increasing network security and decreasing Total Cost of Ownership, where the goal is simple, cost-effective reliability.

FortiOS 5.2 introduced many new features that we will use in this configuration, which is therefore not possible on FortiOS 5.0.x or earlier. The recipe is performed with the FortiGate 1xxD/2xxD series.

By following the recipe, you will be able to provide your small-site customers with simple, yet secure infrastructure that perfectly matches the UTM approach, where we want to centralize as many security features as possible on a single device or cluster.

The recipe provides task-oriented instructions for administrators to fully complete the installation. It is divided into the following sections:

### 1. The Scenario

This section section explains the problems that this new network topology solves, including the cases in which the topology should be used.

### 2. The Topology

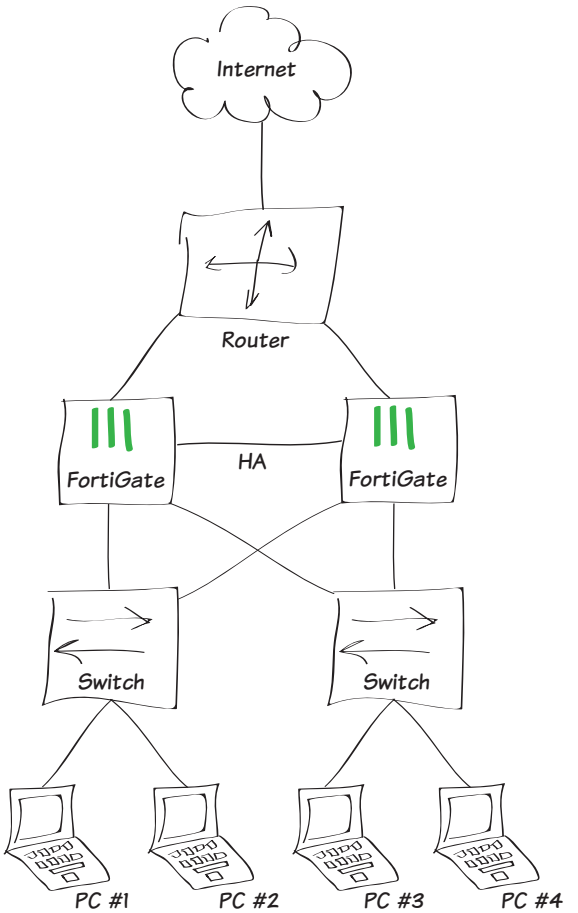
This section includes diagrams of the new topology. It also lists key advantages to this kind of architecture and explains why it solves the problems previously identified in The Scenario.

### 3. Configuration

This section provides step-by-step instructions for configuring the FortiGates within the new topology.

# 1. The Scenario

In the standard scenario, we assume the following topology as the starting point:



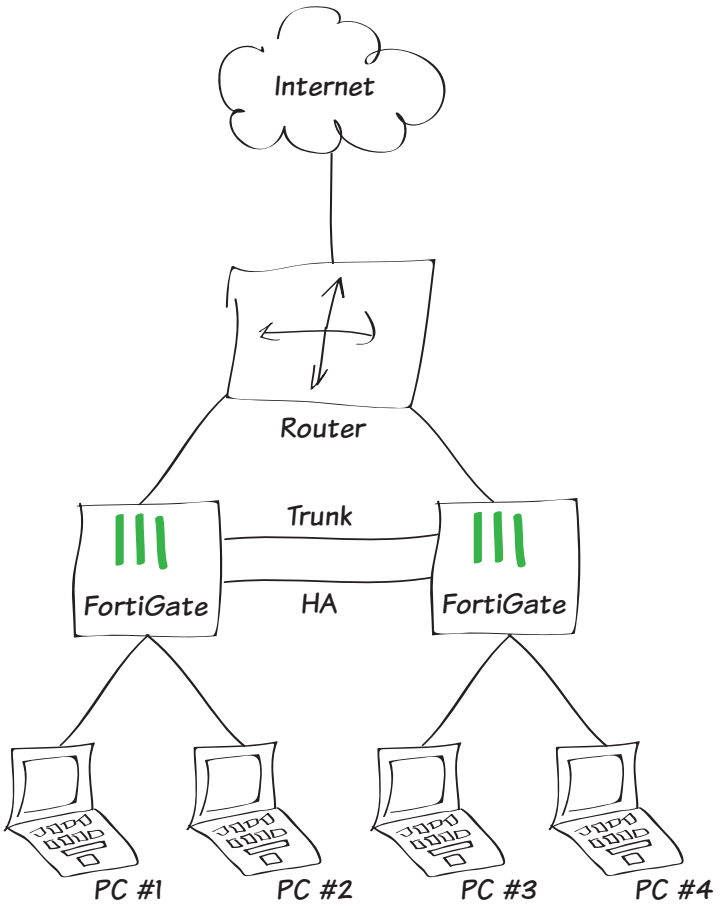

Multi-site customers that want to avoid any “Single Point of Failure” in their remote networks often use this kind of topology. These customers require two FortiGates in Active/Passive mode and therefore two switches on the LAN side to transfer Ethernet payloads to the active FortiGate. There are a few downsides to this approach:

- Four appliances need to be managed and supervised.
- Administrators must know how to work with the Firewall OS and with the Switch OS.
- If one switch fails, the workstations connected won’t be able to reach the Internet.
- Most of the firewall ports are not used.

# 2. The Topology

In this section, we look at the target topology and the scenarios for FortiGate failover. At the end of the section, we discuss the key advantages of adopting the target topology.

## 2.1 The Target Topology



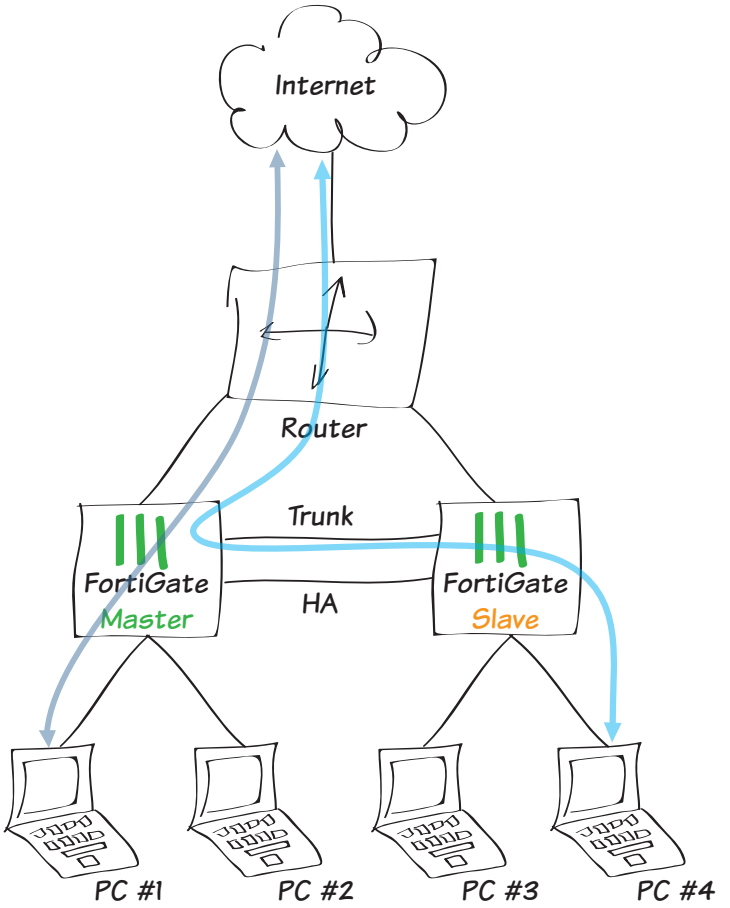

In this new topology, we won't be using additional switches. Instead, we will be using the FortiGate's Integrated Switch Fabric (ISF) solution on both master and slave firewalls.

Note that the target topology uses a FortiGate 2xxD, which has 40 ports. In your configuration, ensure that each FortiGate has enough ports to handle all of the computers in the event of a failover, or switches will still need to be involved.

The administrator will have to configure a trunk link between the two FortiGate physical switches to expand subnets and VLANs from one firewall to the other.

In a FortiGate cluster using FGCP, the slave firewall's ISF can still be used to send traffic destined for the active member across the trunk link.

A representation of the traffic flow appears below:

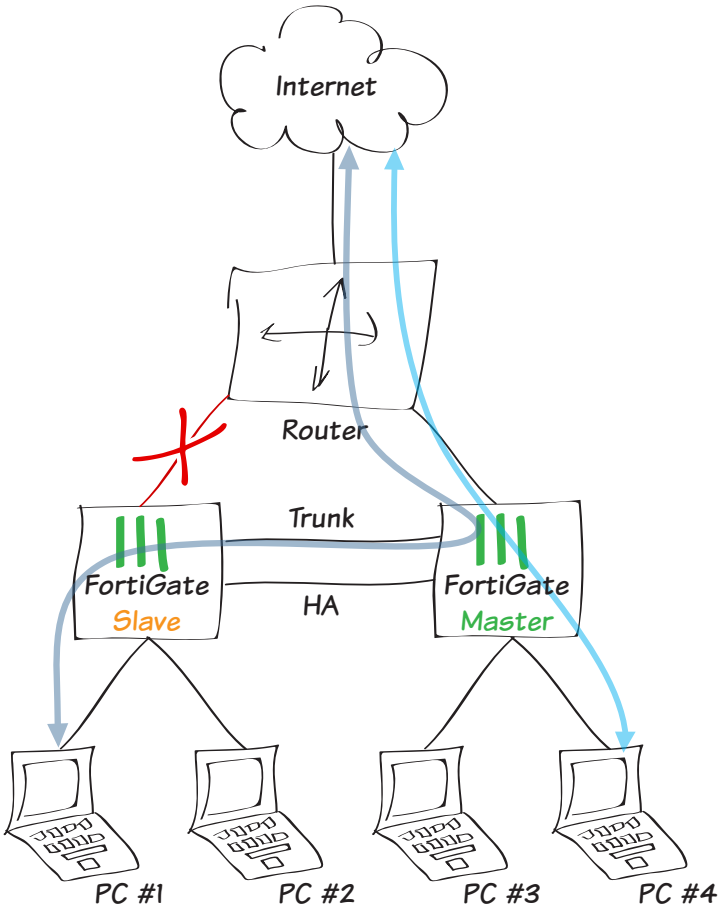


## 2.2 FortiGate Failover

**Case 1: Link failure**

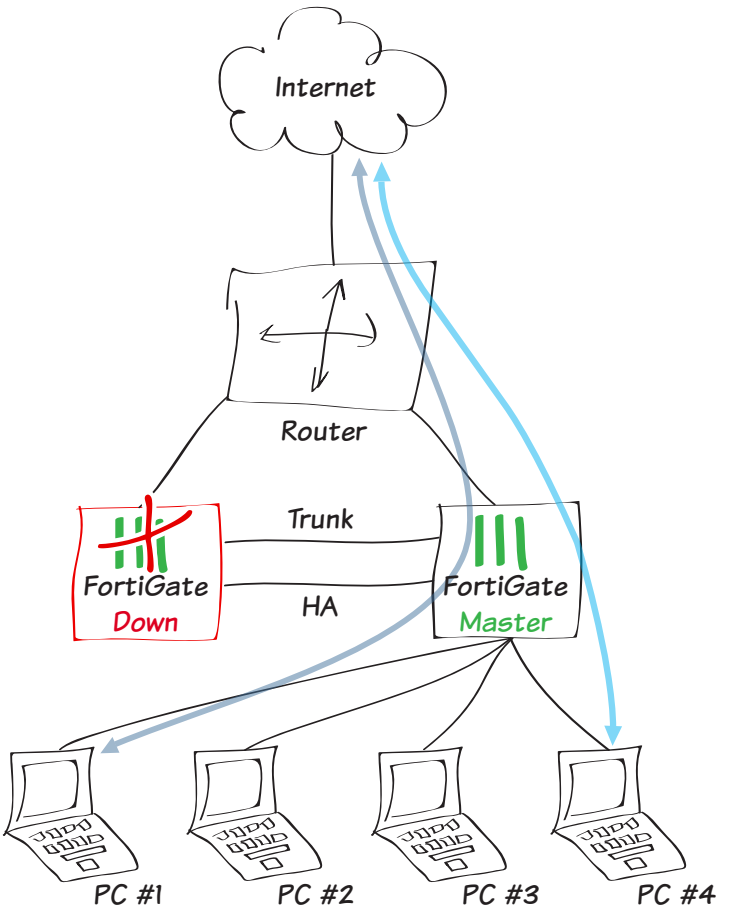
The diagram below represents traffic flow in the event of a failover in the following cases:

- The monitored WAN port, on what was originally the Master FortiGate, fails.
- The link between the router and the original Master FortiGate fails.



**Case 2: FortiGate global failure**

If the master were to completely fail (including the ISF), the administrator would have to plug the LAN segments into the remaining firewall, just as if one switch were to fail in our standard topology.



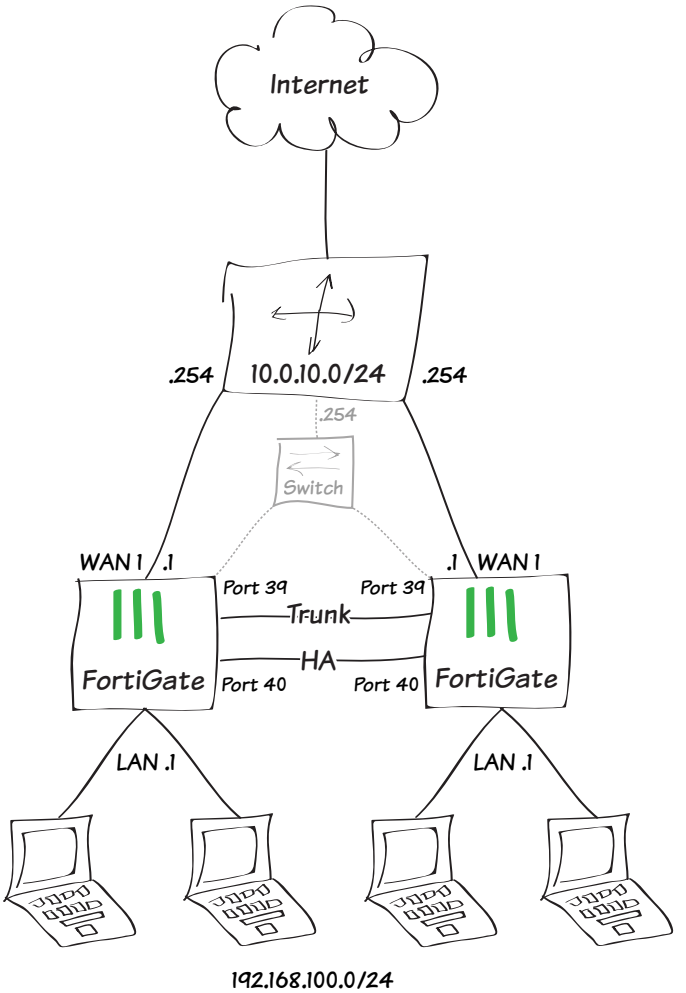

## 2.3 Key Advantages

This new topology offers a few key advantages:

- Only two devices are required, where four are required in the standard topology.
- It is easier for the administrator to manage security and switching on a single device.
- The use of FortiManager simplifies central management.
- There is only one cluster to supervise.

# 3. Configuration

In this section, we reproduce the following network topology. Notice how the router has a switch interface. If your router does not have a switch interface, you will have to add an extra switch (noted in gray below), and in the event of a firewall crash, you will have to power cycle the router.




As we will be changing the configuration of the hardware switch, we strongly recommend that you use the management port to follow the steps below.

By default, the FortiGate management IP address is 192.168.1.99/24.

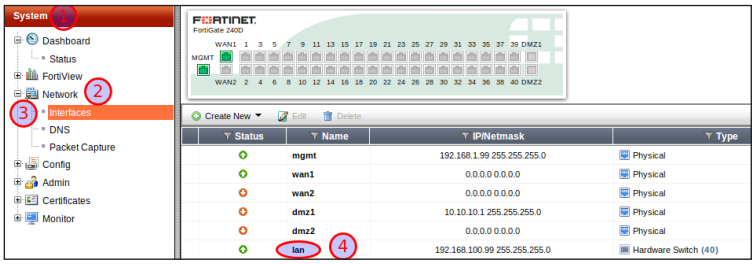
## Step 1: Configure the hardware switch

By default on a FortiGate 1xxD/2xxD, the unit is in Interface mode and all of the internal ports are attached to a hardware switch named **lan**. In this example, we need to use ports 39 and 40 for Trunk and HA respectively.

The first step is to remove ports 39 and 40 from the Hardware Switch lan. Begin by editing the lan interface.

If the unit is in Switch mode, it will have to be reconfigured into Interface mode.

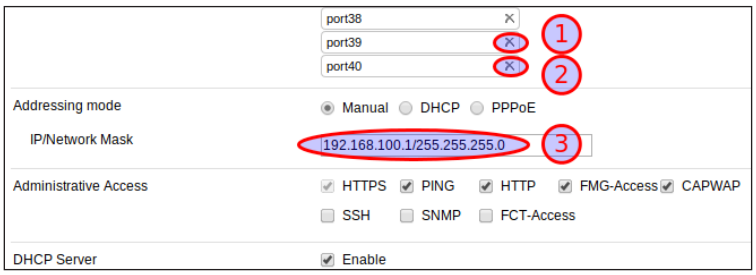
Go to **System** > **Network** > **Interfaces** and double-click **lan** in the interface list.




Remove the last two ports in the list, in this case **port39** and **port40**.

Then configure the **IP/Network Mask** with the following address: **192.168.100.1/255.255.255.0**

When you are done, accept the change.




The interface list should now look like this:

| Status | Name | IP/Netmask | Type |
|---|---|---|---|
| | mgmt | 192.168.1.99 255.255.255.0 | Physical |
| | wan1 | 0.0.0.0 0.0.0.0 | Physical |
| | wan2 | 0.0.0.0 0.0.0.0 | Physical |
| | dmz1 | 10.10.10.1 255.255.255.0 | Physical |
| | dmz2 | 0.0.0.0 0.0.0.0 | Physical |
| | lan | 192.168.100.1 255.255.255.0 | Hardware Switch (38) |
| | port39 | 0.0.0.0 0.0.0.0 | Physical |
| | port40 | 0.0.0.0 0.0.0.0 | Physical |

For the trunk port to work properly, we need to configure a vlan ID on the Virtual Switch. This can only be done in the CLI.

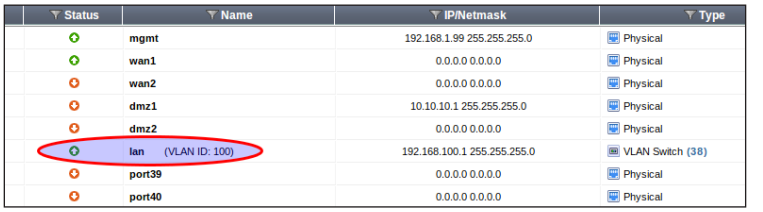
First we need to enable this feature globally. Use the commands shown here:

```
FGT1 # config system global
FGT1 (global) # set virtual-switch-vlan
                enable
FGT1 (global) # end
FGT1 # show system global
config system global
    set fgd-alert-subscription advisory
        latest-threat
    set hostname "FGT1"
    set internal-switch-mode interface
    set optimize antivirus
    set timezone 04
    set virtual-switch-vlan enable
end
```

Next, edit the Virtual Switch and set the vlan number:

```
FGT1 # config system virtual-switch
FGT1 (virtual-switch) # edit lan
FGT1 (lan) # set vlan 100
FGT1 (lan) # end
```

You should now be able to see **VLAN Switch** in the interface list.



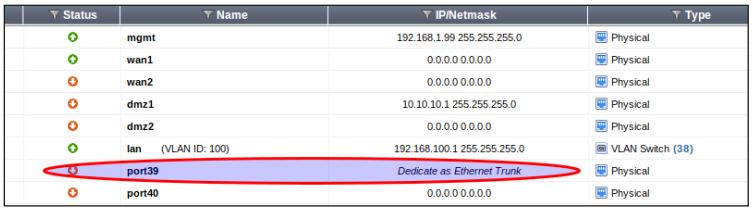

## Step 2: Configure the trunk port

The trunk port will be used to allow traffic to flow between the Virtual Switch of each FortiGate.

Configuring the trunk port is only possible in the CLI:

```
FGT1 # config system interface
FGT1 (interface) # edit port39
FGT1 (port39) # set trunk enable
FGT1 (port39) # end
FGT1 # show system interface port39
config system interface
    edit "port39"
        set vdom "root"
        set type physical
        set trunk enable
        set snmp-index 10
    next
end
```

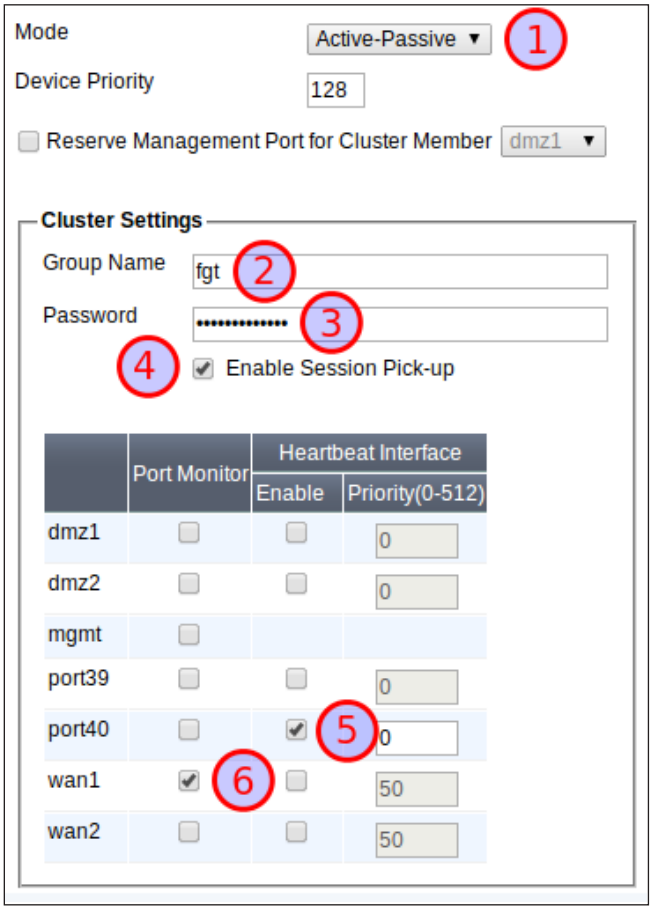
You should now be able to see the trunk port in the interface list.




## Step 3: Configure HA

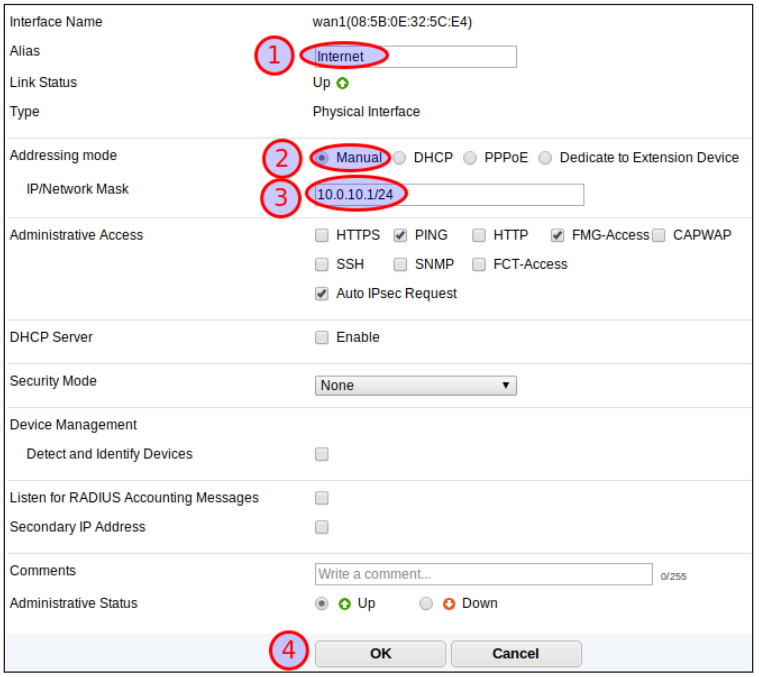
We will now configure High Availability. Port 40 will be used for HeartBeat/Sync communications between cluster members. Port Wan1 will be monitored.

Go to **System** > **Config** > **HA** and configure High Availability as shown:

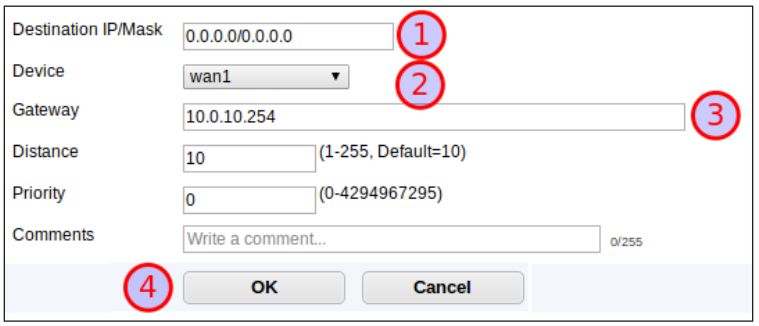


## Step 4: Configure WAN1 IP routing

Go to **System** > **Network** > **Interfaces** and edit **wan1** as shown.




Go to **Router** > **Static** > **Static Routes** and create a new route as shown:

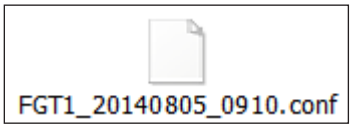



## Step 5: Configure your firewall policies

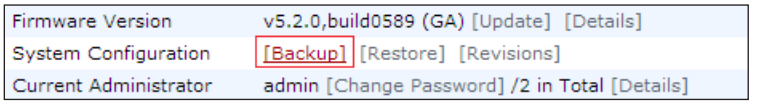
Go to **Policy & Objects** > **Policy** > **IPv4** and configure firewall policies as desired.

## Step 6: Replicate the entire configuration on the second device

Once the first FortiGate is configured, the easiest way to configure the second one is to backup the configuration file of the first FortiGate and restore it on the second.




Go to **System** > **Dashboard** > **Status** and select **Backup** next to **System Configuration** in the 'System Information' panel.




You can change the hostname and HA priority lines directly in the configuration file prior to restoring it on the second FortiGate.

However, do not use a text editor like Notepad or Word to do the editing. Instead, use a code editor like Notepad++ or TextWrangler that won't add unintended content to the file.